UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/899,444	07/05/2001	Elsie Van Herreweghen	CH920000009US1	4090

7590 10/17/2007

Steven Fischman, Esq
SULLY SCOTT MURPHY & PRESSER
400 Garden City Plaza
Suite 300
Garden City, NY 11530-3319

EXAMINER	
KIM, JUNG W	

ART UNIT	PAPER NUMBER
2132	

MAIL DATE	DELIVERY MODE
10/17/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 09/899,444
Filing Date: July 05, 2001
Appellant(s): HERREWEGHEN, ELSIE VAN

John F. Vodopia
Registration No. 36,299
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 8/10/07 appealing from the Office action mailed 1/12/07.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

6,976,162	ELLISON ET AL.	12-2005
6,233,565	LEWIS ET AL.	5-2001

5,850,442	MUFTIC	12-1998
5,604,805	BRAND	2-1997

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 103

Claims 6-11, 13, 17, 19-22, 25-28, 31, 32, 34 and 35 are rejected under 35 U.S.C. 102(e) as being unpatentable over Lewis et al. U.S. Patent No. 6,233,565 (hereinafter Lewis) in view of Ellison et al. USPN 6,976,162 (hereinafter Ellison) and Brand USPN 5,604,805 (hereinafter Brand).

As per claim 6, Lewis discloses a receipt generation method, comprising generating an electronic receipt in a communication system providing a public key encryption system, including the steps of:

a. receiving a message from a sender, the message is electronically signed by the sender using a private signature key owned by the sender, whereby the message includes a transaction request and a reference to a designated owner of a receipt to be generated (Lewis, col. 4:20-27; cols. 7 and 8, TABLE 1, "Transaction Type");

b. authenticating the message using a public signature verification key associated to the private signature key held by the sender of the message (Lewis, 4:24-27; cols. 7 and 8: TABLE 1 under "Transaction Type":

"authentication client 2n to server", under "Transaction Server 190" and "Master Server 300");

c. issuing a receipt including the reference to the designated owner of the receipt and details for what the receipt has been given to provide the designated owner with the receipt (Lewis, 4:32-38); and

d. electronically signing the receipt with the public signature key assigned to an issuer issuing the receipt (Lewis, 4:41-44).

Lewis does not teach using a pseudonym on the message from the sender, wherein the pseudonym is issued using a first private-public key pair, and the receipt enables the owner to verify ownership of the receipt while maintaining the owner anonymous or pseudonymous. Ellison discloses producing pseudonyms by generating a key pair and certifying the generated public key by a trusted center to withhold the identity of a user in transactions requiring the use of the pseudonym key to certify digital signatures of the user (Ellison, col. 3:8-13; 3:57-5:9). In the method of Lewis, the public/private keys used to sign and verify the signatures of the receipts are rendered anonymous using the anonymous keys as taught by Ellison. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to verify ownership of the receipt while maintaining the anonymity of the owner of the receipt, since it is desirous to maintain the privacy of a user transferring certified information (Ellison, 1:65-2:1).

Finally, Lewis does not disclose using a second private-public signature key pair different than the first private-public signature key pair to verify the ownership of the receipt. Brand discloses a cryptographic concept of using different pseudonyms at different organizations such that the pseudonyms are unlinkable. (col. 2:15-34) This concept as applied to the teachings of Lewis and Ellison suggest using different pseudonym key pairs for different types of transactions to ensure unlinkablity of the transaction between the user and the organization issuing the receipt, and the transaction between the user and the organization verifying the receipt. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to use a second private-public signature key pair different than the first private-public signature key pair to verify the ownership of the receipt, while maintaining the owner anonymous or pseudonymous. This would ensure better privacy for the user since the organization generating the receipt and the organization validating the ownership of the receipt are not able to collude to identify the owner of the receipt, Brand, ibid. The aforementioned cover the limitations of claim 6.

As per claim 7, the rejection of claim 6 under 35 U.S.C. 103(a) is incorporated herein. (supra) In addition, the method further includes the steps of performing the requested transaction, and returning the receipt to the sender (Lewis, col. 4:32-33).

As per claims 8-10, the rejection of claim 6 under 35 U.S.C. 103(a) is incorporated herein. (supra) In addition, Ellison discloses using a pseudonym for communicating and using a pseudonym as a reference to a designated owner (Ellison, col. 1:65-2:1; Abstract). It would be obvious to one of ordinary skill in the art at the time the invention was made to use a pseudonym for communication and designating the owner with a pseudonym to be used as a reference to the owner since it is desirous to maintain the privacy of a user transferring certified information (Ellison, ibid). Further, an anonymous communication connection is necessarily required in a pseudonym protocol. The aforementioned cover the limitations of claims 8-10.

As per claim 11, the rejection of claim 6 under 35 U.S.C. 103(a) is incorporated herein. (supra) In addition, the designated owner of the receipt is the sender (Lewis, col. 4:32-35).

As per claim 13, the rejections of claims 7 and 11 under 35 U.S.C. 103(a) are incorporated herein. In addition, the method disclosed by Lewis is also a method of proving ownership of a receipt (holder of the digital receipt signed by both the owner and the issuer proves ownership of the receipt) including the steps of:

e. a user using a pseudonym to create a first message including a transaction request and a reference to a designated owner of a receipt to be generated in response to receiving the message, wherein the pseudonym is issued to the user using a first private-public signature key pair (Lewis, col. 4:20-27; the sender of the transaction request is the designated owner of the receipt; Ellison, 4:10-14);

f. the user electronically signing the message using the first private signature key (Lewis, 4:24-25; cols. 7 and 8: TABLE 1 under "Transaction Type": "authentication client 2n to server");

g. sending the first message to a first addressee (Lewis, 4:20-27; first addressee is the transaction server; and

h. receiving the receipt from the first addressee, the receipt being electronically signed by the first addressee using a second private signature key of a second private-public key pair assigned to the first addressee, wherein the receipt includes information as for what the receipt has been issued and the reference to the designated owner of the receipt and thereby to enable the owner to verify ownership of the receipt by using the second private-public signature key pair different then the first private-public signature key pair while maintaining the owner anonymous or pseudonymous (Lewis, 4:32-43 [the receipt comprises the client digital signature and the server digital signature, which generated the receipt]; Ellison, 3:8-13; 3:57-5:9 [digital signature created by pseudonym public key]).

It would be obvious to one of ordinary skill in the art at the time the invention was made to maintain the anonymity of the owner, since it is desirous to maintain the privacy of a user transferring certified information (Ellison, col. 65-2:1). The aforementioned cover the limitations of claim 13.

As per claim 17, the rejection of claim 13 under 35 U.S.C. 103(a) is incorporated herein. (supra) In addition, the reference to the designated owner of the receipt is a pseudonym used by the owner of the receipt (Lewis, 4:32-34 [the receipt comprises the client's digital signature]; Ellison, col. 3:8-13; 3:57-5:9 9 [digital signature created by pseudonym public key]). It would be obvious to one of ordinary skill in the art at the time the invention was made for the reference to the designated owner of the receipt to be a pseudonym used by the owner of the receipt, since it is desirous to maintain the privacy of a user transferring certified information (Ellison, col. 1:65-2:1). The aforementioned cover the limitation of claim 17.

As per claim 19, the rejection of claim 13 under 35 U.S.C. 103(a) is incorporated herein. (supra) In addition, the designated owner of the receipt is identical to a sender sending the first message to the first addressee (Lewis, col. 4, 20-27 [the sender of the transaction request is the designated owner of the receipt]).

As per claim 20, the rejections of claims 13 and 19 under 35 U.S.C. 103(a) are incorporated herein. In addition, the method further comprises creating a second message including the receipt; electronically signing the second message using a second private signature key; and sending the second message to the designated owner of the receipt (Lewis, col. 4:32-43).

As per claims 21 and 22, the rejection of claim 20 under 35 U.S.C. 103(a) is incorporated herein. In addition, Ellison discloses using pseudonyms to withhold the identity of a user in transactions requiring the use of certifying a signature, wherein the signature remains anonymous (col. 3:8-13; 3:57-5:9). It would be obvious to one of ordinary skill in the art at the time the invention was made wherein the sending and receiving of the first and second messages are performed by using a pseudonym, since it is desirous to maintain the privacy of a user transferring certified information (Ellison, 1:65-2:1). Finally, an anonymous communication connection is necessarily required in a pseudonym protocol. The aforementioned cover the limitations of claims 21 and 22.

As per claims 25 and 26, they are apparatus claims corresponding to claims 6 and 13, and they do not teach or define above the information claimed in claims 6 and 13. Therefore, claims 25 and 26 are rejected as being unpatentable over Lewis in view of Ellison and Brand for the same reasons set forth in the rejections of claims 6 and 13.

As per claims 27, 28, 31 and 32, the rejections of claims 6 and 13 under 35 U.S.C. 103(a) are incorporated herein. (supra) In addition, means to perform the methods of claims 6 and 13 are embodied in a program of instructions executable by a machine (Lewis, Figure 2).

As per claims 34 and 35, the rejections of claims 6, 13, 25, 26, 27, 28, 31 and 32 under 35 U.S.C. 103(a) are incorporated herein. (supra) In addition, means to affect the functions of the devices of claims 25 and 26 comprise computer readable program (Lewis, col. 2:10-14).

Claims 1-5, 23, 24, 30 and 33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lewis in view of Muftic U.S. Patent No. 5,850,442 (hereinafter Muftic) and Ellison.

As per claims 1-4, Lewis discloses a method comprising generating an electronic receipt in a communication system providing a public key encryption infrastructure, wherein a server generation module in response to an electronic payment transaction, generates a receipt and transmits the receipt, wherein the receipt comprises a client digital signature and a server digital signature, and a data set uniquely identifying the executed transaction, wherein the receipt authenticates the electronic transaction, and the receipt includes details for what the receipt has been given and a reference to a designated owner (Lewis, col. 4:24-44). Lewis does not expressly teach how the electronic receipt is authenticated. Muftic teaches an ordinary means of authenticating a signed message by a sender of the message using a public key encryption infrastructure including the following steps:

i. receiving a message from a sender, the message being electronically signed by the sender using a private signature key owned by the sender; the corresponding public key of the sender is provided within a digital certificate by a trusted issuer and signed by the issuer having given the certificate, wherein the certificate includes details for the context of the certificate and a reference to the owner of the certificate (Muftic, col. 2:42-51; 3:35-52; 4:27-32; digital certificates in the standard X.509 define attributes including certificate context and key subscriber identity values);

j. obtaining a public signature verification key on the basis of the reference to the owner of the certificate (digital certificates enables trusted retrieval of the public signature verification key); and

k. examining whether or not the private signature key used for electronically signing the message is associated to the public signature verification key obtained on the basis of the reference to the owner of the certificate (Muftic, 2:44-51).

Although Muftic does not expressly teach submitting the certificate holding the public signature verification key and signed by the issuer with the original signed message, the step of including the certificate with the signed message is a trivial combination since proper verification of the signed message requires the signed certificate (see Muftic, 3:30-33); moreover, the combination of disparate parts has been found to be an obvious feature. See In re Larson 144 USPQ 347 (CCPA 1965). Further, the digital certificate taught by Muftic is operatively equivalent to the electronic receipt: both maintain a record of an agreement/transaction between the owner and the issuer. Hence, it would be obvious to one of ordinary skill in the art at the time the invention was made to verify the receipt according to the recited steps of applicant's claim 1, since it is desirous to cryptographically verify the receipt as being owned by the sender and issued by the issuer (Lewis, 4:36-38; Muftic, 2:10-14 and 3:47-49).

Finally, Lewis does not teach the reference to the owner of the receipt is a pseudonym used by the owner of the receipt, wherein a certificate securely links the pseudonym to the public signature verification key, such that verification of ownership of the receipt is enabled while maintaining the owner anonymous or pseudonymous. Ellison discloses creating user pseudonyms by generating a key pair and certifying the generated public key by a trusted center to withhold the identity of a user in transactions requiring the use of the pseudonym key to certify digital signatures of the user, (Ellison, col. 3:8-13; 3:57-5:9). In the method of Lewis, the keys used to sign and to verify the signatures of the receipts are rendered anonymous using the anonymous keys as taught by Ellison. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made for the reference to the owner of the receipt to be a pseudonym used by the owner of the receipt and a certificate to securely link the pseudonym to the public signature verification key, such that verification of ownership of the receipt is enabled while maintaining the owner anonymous or pseudonymous, since it is desirous to maintain the privacy of a user transferring certified information (Ellison, 1:65-2:1). The aforementioned cover the limitations of claims 1-4.

As per claim 5, the rejection of claim 1 under 35 U.S.C. 103(a) is incorporated herein. (supra) In addition, the method further comprises the step of authenticating the receipt using a public signature verification key assigned to the issuer of the receipt (Lewis, col. 4:24-44; Muftic, col. 3:44-52).

As per claim 24, it is an apparatus claims corresponding to claim 1, and it does not teach or define above the information claimed in claim 1. Therefore, claim 24 is rejected as being unpatentable over Lewis in view of Muftic and Ellison for the same reasons set forth in the rejection of claim 1.

As per claims 23 and 30, the rejections of claims 1 and 24 under 35 U.S.C. 103(a) are incorporated herein. (supra) In addition, means to perform the method of claim 1 is embodied in a program of instructions executable by a machine (Lewis, Figure 2).

As per claim 33, the rejections of claims 1, 23, 24 and 30 under 35 U.S.C. 103(a) are incorporated herein. (supra) In addition, means to affect the functions of the device of claim 24 comprise a computer readable program (Lewis, col. 2:10-14).

Claims 12, 14-16 and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lewis in view of Ellison, Brand and Muftic.

As per claim 12, the rejection of claim 6 under 35 U.S.C. 103(a) is incorporated herein. (supra) Lewis does not expressly disclose the reference to a designated owner is a public signature key associated to a private signature verification key held by the designated owner of the receipt. (Lewis discloses the receipt comprises a client digital signature and a data set uniquely identifying the executed transaction) However, a public signature key as the reference to a designated owner is an obvious enhancement because it uniquely identifies the corresponding private signature key used to sign the receipt. As disclosed by Muftic, public keys are conventionally certified by means of a certificate to associate a signature key with a subscriber (col. 2:42-51; 3:35-52; 4:27-32). Hence, it would be obvious to one of ordinary skill in the art at the time the invention was made for the reference to a designated owner to be a public signature key associated to a private signature verification key held by the designated owner of the receipt, because it enables a certified reference to the signed receipt. The aforementioned cover the limitations of claim 12.

Regarding claims 14, 15 and 18, the rejection of claim 13 under 35 U.S.C. 103(a) is incorporated herein. (supra) Lewis does not expressly teach creating a second message including the receipt to authenticate the receipt. Muftic teaches an ordinary means of authenticating a signed message by a sender of the message using a public key encryption infrastructure including the following steps:

I. receiving a message from a sender, the message being electronically signed by the sender using a private signature key owned by the sender; the corresponding public key of the sender is provided within a digital certificate by a trusted issuer and signed by the issuer having given the certificate, wherein the certificate includes details for the context of the certificate and a reference to the owner of the certificate (Muftic, col. 2:42-51; 3:35-52; 4:27-32; digital certificates in the standard X.509 define attributes including certificate context and key subscriber identity values);

m. obtaining a public signature verification key on the basis of the reference to the owner of the certificate (digital certificates enables trusted retrieval of the public signature verification key); and

n. examining whether or not the private signature key used for electronically signing the message is associated to the public signature verification key obtained on the basis of the reference to the owner of the certificate (Muftic, 2:44-51).

Although Muftic does not expressly teach submitting the certificate holding the public signature verification key and signed by the issuer with the original signed message, the step of including the certificate with the signed message is a trivial combination since proper verification of the signed message requires the signed certificate (see Muftic, 3:30-33); moreover, the combination of disparate parts has been found to be an obvious feature. See In re Larson 144 USPQ 347 (CCPA 1965). Further, the digital certificate taught by Muftic is operatively equivalent to the electronic receipt: both maintain a record of an agreement/transaction between the owner and the issuer. Hence, it would be obvious to one of ordinary skill in the art at the time the invention was made to verify the receipt according to the recited steps of applicant's claim 14 and 18, since it is desirous to cryptographically verify the receipt as being owned by the sender and issued by the issuer (Lewis, 4:36-38; Muftic, 2:10-14 and 3:47-49). Finally, the user signs the first and second messages using their private signature key, hence, the first private signature key is identical to the second private signature key. The aforementioned cover the limitations of claims 14, 16 and 18.

As per claim 15, the rejection of claim 14 under 35 U.S.C. 103(a) is incorporated herein. (supra) Lewis does not expressly teach the first addressee is identical to the second addressee. However, it is notoriously well known for certification parties who issue certificates also verify the certificates. For example, trusted certification issuers such as VeriSign both issue certificates and verify issued certificates. Examiner takes Official Notice of this teaching. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made for the first addressee to be identical to the second addressee since a single party may be best equipped to handle both roles as known to one of ordinary skill in the art. Furthermore, it is desirable for a server issuing a receipt to be able to validate the receipt, since a receipt acts as a record of services requested and paid for by the user. The aforementioned cover the limitations of claim 15.

(10) Response to Argument

With respect to Appellant's arguments that the 103(a) rejections under Lewis, Ellison and Brand do not provide adequate motivation to combine the prior art of Lewis, Ellison and Brand, and, assuming that the combination is proper, do not disclose all limitations of the respective claims (Brief, pgs. 8-11), these arguments are deficient for the following reasons. As indicated in the rejections of the final Office action mailed on 1/12/07, Lewis discloses a method for Internet-based financial transactions comprising the steps of receiving a request to generate a certified receipt, whereby the request is signed using a client signature key (public-private key) and signing the generated receipt using an issuer's signature key (public-private key) (col. 4:20-27 and lines 40-44; 5:10-25). As known in the art, digital signatures provide cryptographically secure authentication means for an electronic datum. In the invention of Lewis, the digital signature of the sender validates the sender as the author of the message and validates the integrity of the sender's message; and, likewise, the digital signature of the issuer validates the issuer as the author of the receipt and validates the integrity of the receipt. Ellison discloses producing pseudonyms by generating an anonymous public-private key pair and certifying the generated public key by a trusted certifying authority to ensure that only the trusted certifying authority and the user know that the signature key identifies the user, thereby withholding the identity of the user in electronic transactions with third parties (Ellison, col. 3:8-13; 3:57-5:9). Ellison explicitly identifies using pseudonyms by a user to prevent identity-based attacks based on vulnerabilities in electronic commerce and business-to-business transactions (col. 1:12-49 and 1:66-2:1; 3:58-64). Hence, Lewis in view of Ellison suggests using a pseudonym public key to sign the various transactions that require certification of the respective parties; such transactions encompass electronically transmitted financial messages and any residual artifacts that identify the participants, including receipts. Furthermore, Brand discloses using different pseudonyms by a user with different organizations such that the pseudonyms are unlinkable (col. 2:15-34). This particular concept of Brand applied to the teachings of Lewis and Ellison suggest using different pseudonym key pairs for different types of transactions to ensure unlinkability of the transaction between a user and the organization issuing the receipt, and between the user (owner of the receipt) and the organization verifying the receipt. Such a configuration renders obvious the feature of using a first and a second private-public key pair to render anonymous the various transactions as claimed by Appellant. Therefore, contrary to Appellant's allegations, Lewis, Ellison and Brand in combination suggest all limitations of the claims in question.

With respect to Appellant's arguments that the 103(a) rejections under Lewis, Muftic and Ellison do not provide adequate motivation to combine the prior art of Lewis, Muftic and Ellison, and, assuming that the combination is proper, do not disclose all limitations of the respective claims (Brief, pgs. 12-14), these arguments are deficient for the following reasons. As indicated in the rejections of the final Office action mailed on 1/12/07, Lewis discloses a method for Internet-based financial transactions comprising the steps of generating an electronic receipt in a communication system providing a public key encryption infrastructure, wherein a server generation module, in response to an electronic payment transaction, generates a receipt having a client digital signature, server digital signature, information identifying for what the receipt has been given, a reference to a designed owner of the receipt, and a data set uniquely identifying the executed transaction, such that the receipt authenticates the electronic transaction; and transmitting the receipt as a result of an electronic payment (Lewis, col. 4:24-44). Muftic discloses standard means of authenticating a signed message by a sender of the message using a public key encryption infrastructure, whereby a public key is first distributed using a digital certificate and then used to verify the authenticity of a message signed with the corresponding private key (col. 2:42-51; 3:35-52; 4:27-32; X.509 protocol). Moreover, because digital certificates are themselves certified by a trusted public entity, whereby the trusted public entity signs the entire contents of the certificate (X.509 protocol certificates includes the public key, an issuer identifier, a subject identifier, and an issuer's signature over a hash of the certificate), the certificate cannot be tampered with without exposing the offensive act. This essentially provides a secure container for a public key to ensure the validity of the key and other relevant information including the subject to whom the key refers, regardless of who possessed the digital certificate at any point in time after the distribution of the certificate. Hence, the teaching of Muftic as applied to the invention of Lewis suggests verifying a receipt signed with a private key by using a corresponding public key obtained via a digital certificate, because it is desirous to cryptographically verify the receipt as being owned by the sender, and to ensure that the means to verify the receipt has not been compromised (Lewis, 4:36-38; Muftic, 2:10-14 and 3:47-49). Finally, Ellison discloses producing pseudonyms by generating an anonymous public-private key pair and certifying the generated public key by a trusted certifying authority to ensure that only the trusted certifying authority and the user know that the signature key identifies the user, thereby withholding the identity of the user in electronic transactions with third parties (Ellison, col. 3:8-13; 3:57-5:9). Ellison explicitly identifies using pseudonyms by a user to prevent identity-based attacks based on vulnerabilities in electronic commerce and business-to-business transactions (col. 1:12-49 and 1:66-2:1; 3:58-64). Hence, Lewis and Muftic in view of Ellison suggests using a pseudonym public key to sign the various transactions that require certification of the respective parties; such transactions encompass electronically transmitted financial messages and any residual artifacts that identify the participants, including receipts. Therefore, contrary to Appellant's allegations, Lewis, Ellison and Brand in combination suggest all limitations of the claims in question.

With respect to Appellant's arguments that the 103(a) rejections under Lewis, Ellison, Brand and Muftic do not provide adequate motivation to combine the prior art of Lewis, Ellison, Brand and Muftic, and assuming that the combination is proper, do not disclose all limitations of the respective claims (Brief, pgs. 15-16), these arguments are deficient for substantially the same reasons articulated above. Contrary to Appellant's allegations (see pg. 16, 1st full paragraph), Lewis's disclosure teaches issuing and verifying ownership of a receipt via public keys signatures; Ellison discloses maintaining a user anonymous or pseudonymous via pseudonymous public keys to prevent identity-based attacks; Brands discloses using different signing key pseudonyms to prevent transactions by a user from being linked; and Brands as applied to the teachings of Lewis and Ellison disclose a user and receipt issuer exchanging information using a first private-public key pair, and the receipt issuer and owner communicating using a second private-key pair. Finally, Muftic discloses standard means of authenticating a signed message by a sender of the message using public key encryption infrastructure to ensure cryptographically secure authentication measures. Therefore, Lewis, Ellison, Brand and Muftic in combination suggest all limitations of the claims in question.

For the above reasons, it is believed that the rejections should be sustained.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

Respectfully submitted,

GILBERTO BARRÓN JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

Jung Kim
Examiner, AU 2132

Conferees:

Gilberto Barron
SPE AU 2132

Matthew Smithers

/Matthew Smithers/
Primary Examiner, AU 2137